FBIM Transactions
DOI 10.12709/fbim.04.04.02.16

NEKI RIZICI KOD ZAŠTITE PODATAKA O LIČNOSTI I MOGUĆNOSTI NJIHOVE ELIMINACIJE

SOME RISKS IN THE PROTECTION OF PERSONAL DATA AND THE POSSIBILITIES OF THEIR ELIMINATION

Draško Šćekić
Fakultet za poslovno industrijski menadžment „Union – Nikola Tesla" Univerziteta, Beograd, Srbija

JEL kategorija: **D82, K36, Y9**

Apstrakt

Pravo na privatnost predstavlja jedno od osnovnih ljudskih prava tako da mu se u čitavom svetu poklanja pažnja koja je srazmerna razvijenosti društva na konkretnom području. Podaci o ličnosti su jedan od suštinskih elemenata na kome se temelji ovo pravo i njihova zaštita iskazuje meru u kojoj je ono ispoštovano. Ubrzani razvoj informaciono komunikacionih tehnologija doveo je do korišćenja i obrade podataka o ličnosti u svim sferama svakodnevnog života što posledično uzrokuje stalni porast njihovog opšteg značaja i važnosti u životu svakog pojedinca. Time su rizici od zlouptrebe podataka o ličnosti enormno narasli zbog čega ih je veoma teško i u razvijenim zemljama držati u granicama koje se mogu tolerisati. Ograničavanje i suzbijanje rizika je veoma složen proces sa kojim se mora suočiti i u kontinuitetu baviti svaka zemlja ukoliko ima pretenzije da napreduje i uskladi svoj razvoj sa savremenim tokovima u svetu. Cilj rada je da pokaže kakva je trenutna situacija u Srbiji kroz jednu visokoprofitabilnu delatnost u kojoj je svakodnevna pojava prikupljanje i obrada podataka o ličnosti.

Ključne reči: *Podaci o ličnosti, pravo na privatnost, rizik, zloupotreba, zaštita, studija uticaja na privatnost, izveštaj o etici*

Abstract

The right to privacy is one of the basic human rights to whom, in the whole world, is payed attention which is proportional to the development of the society in a concrete area. Personal data are one of the essential elements on which is based this human right and their protection shows how much is that respected. The rapid development of information and communication technologies has led to the using and processing of personal data in all areas of

Adresa autora:
Draško Šćekić
draskos@telekom.rs

everyday life, which causes a steady increase in their overall significance and importance in the life of every individual. Consequently, the risk of misuse of personal data is grown enormously and it is very difficult, even in the developed countries, to keep it within the limits that can be tolerated. The risk limiting and decreasing are very complex processes. Each country is faced to these challenges if it intends to harmonize its development with the latest developments in the world. This article aims to present the current situation in Serbia through one highly profitable industry in which a collecting and processing of personal data are everyday activities.

***Keywords**: Personal data, right to privacy, risk, misuse, protection, privacy impact assessment, ethics*

1 UVOD

Član 3, tačka 1 Zakona o zaštiti podataka o ličnosti Republike Srbije (2008) glasi: „Podatak o ličnosti je svaka informacija koja se odnosi na fizičko lice, bez obzira na oblik u kome je izražena i na nosač informacije (papir, traka, film, elektronski medij i slično) po čijem nalogu, u čije ime, odnosno za čiji račun je informacija pohranjena, datum nastanka informacije, mesto pohranjivanja informacije, način saznavanja informacije (neposredno, putem slušanja, gledanja i slično, odnosno posredno, putem uvida u dokument u kojem je informacija sadržana i slično), ili bez obzira na drugo svojstvo informacije (u daljem tekstu: podatak).“ Konkretno podaci o ličnosti su:

- Prezime i ime
- JMBG (Jedinstveni matični broj građana)
- Datum i mesto rođenja
- Državljanstvo
- Zaposlenje
- Funkcija, položaj i status
- Adresa
- Broj telefona
- Broj lične karte
- Broj pasoša
- Broj studentskog indeksa
- Broj zdravstvenog osiguranja
- Poreski broj.

U podatke o ličnosti se mogu ubrojati i biometrijske odlike glas, slika, krvna grupa, otisak prsta, otisak uva, otisak mrežnjače, DNK, zatim osetljiva obeležja rasa, nacionalnost, veroispovest, jezik, pol, politička opredeljenost, zdravstveno stanje, finansijsko stanje, članstvo u organizacijama, presude, seksualni život kao i svaki drugi podatak na osnovu koga pojedinac može biti identifikovan odnosno izložen zloupotrebi ili maltretiranju. Zato je zaštita ovih podataka neraskidivi deo progresa kojeg donosi informaciono društvo. Ona se ne može ograničiti samo na usklađivanje sa zakonima koji se odnose na ovu problematiku. Pored toga moraju se koristiti sva najsavremenija tehnička i tehnološka dostignuća pri čemu se opet neće zaokružiti ovaj proces. Za tako nešto neophodno je primenjivati neke novije koncepte, kao što je PbD (Privacy by Design-Integrisana zaštita privatnosti), koji donose sasvim drugačije načine razmišljanja u odnosu na tradicionalne. (Cavoukian, 2011)

To znači da zaštita privatnosti treba biti implementirana u svaku poru organizacije ili poslovnog sistema ili prosto rečeno mora biti podrazumevani oblik rada. U savremenom poslovanju ona se začinje sa organizacijskom kulturom i sa njom se razvija. Ima svoj životni ciklus koji počinje onog momenta kada se prvi podatak prikupi, zatim živi tokom obrade, upotrebe i čuvanja podataka i traje do njihovog brisanja. Zaštita podataka o ličnosti predstavlja kontinuiran i sistematičan proces, jer se mora stalno usklađivati, prilagođavati, unapređivati i razvijati. Zato su danas stručnjaci skoncentrisani na iznalaženje rešenja koja omogućavaju sistematičan pristup zaštiti podataka. (Zajić, 2015)

Odvija se kroz stalno i naporno „nadmetanje” koje ima za cilj da obezbedi dugoročni uspeh i trajnu prevagu u tom pogledu. Naime, potreba informacionog društva za obrazovanjem sve većeg broja stručnjaka u oblasti informatike stvara potencijalno vrlo izvesnu latentnu opasnost za usmeravanje znanja u suprotnom smeru od željenog. Takođe i brzi razvoj informaciono komunikacionih tehnologija direktno utiče na to da se svaki diskontinuitet po pitanju njegovog praćenja, kao veoma kompleksnog i krajnje zahtevnog procesa, reflektuje kroz nagli rast rizika koji ga prate. Posledično dolazi do njegovog

usložnjavanja pa se pred poslovnim sistemima koji generišu zbirke ili baze podataka o ličnosti postavljaju sve složeniji zahtevi kada je u pitanju upravljanje ili rukovanje istima.

2 RIZICI I POSLEDICE

Rad sa podacima o ličnosti, kao što je rečeno, pretpostavlja po automatizmu i njihovu zaštitu, koja se odvija kroz više faza od kojih su sledeće jasno definisane i lako prepoznatljive:

– razmatranje svrhe obrade,
– prepoznavanje rizika,
– procena rizika i
– mere za umanjenje rizika.

Zakonom o zaštiti podataka o ličnosti Republike Srbije (2008) i njegovim članovima 8-18 regulisani su uslovi pod kojima se neko može baviti prikupljanjem, obradom, korišćenjem i čuvanjem podataka o ličnosti. Ovaj zakon, koji je trenutno važeći u RS, u međuvremenu je imao toliko beznačajne izmene da ih nema svrhe uzimati u obzir. Od njegovog stupanja na snagu proteklo je više od 6 godina, što u razvoju IK tehnologija predstavlja veoma značajan, pa i dug, period. Ovaj podatak nas na samom početku upućuje na pretpostavku da zaštita podataka o ličnosti u pravnom smislu još nema tretman kakav joj treba posvećivati. Naravno da to posledično utiče da se obaveze i odgovornosti rukovalaca zbirkama podataka o ličnosti ne nadograđuju, usavršavaju i u svakom pogledu povećavaju. O tome nam svedoči i veoma kritična ili bolje rečeno haotična situacija u pojedinim oblastima, od kojih kao reprezentativan primer možemo uzeti video nadzor. Zakon o zaštiti podataka o ličnosti uopšte nema odredaba koje se odnose na aktivnosti u ovom segmentu naprednih tehnologija. Na taj način je u velikoj meri ugroženo pravo na privatnost s obzirom na instaliranje i upotrebu opreme iz ovog domena svuda u okruženju (na iole bitnim lokacijama) i praćenje istom u realnom vremenu (tokom 24 sata) bez ikakvih ograničenja i kontrola, najčešće od lica koja za takvu aktivnost nemaju nikakva ovlašćenja.

I ne samo da je ugroženo pravo na privatnost već je ugrožena i bezbednost postojećih zbirki podataka o ličnosti, koje imaju izgrađenu i stalno prisutnu zašitu. Ako se njihova zaštita temelji recimo na otisku prsta ili mrežnjače, moguće je sa opremom visoke tehnologije kao što su kamere visoke rezolucije, zastupljene čak i na mobilnim telefonskim aparatima, izvršiti skeniranje navedenih elemenata i učiniti te zbirke podataka o ličnosti dostupnim za raznovrsne oblike zloupotreba.

Rizici koji se mogu javiti u radu sa podacima o ličnosti, na osnovu posledica ili šteta koje mogu prouzrokovati, mogu se svrstati u one koji se odnose na pojedinca i one koji se odnose na organizaciju. Prvi se generišu usled mogućnosti gubitka, uništenja ili zloupotrebe podataka pojedinca i u krajnjem slučaju bivaju izraženi stepenom narušavanja njegovog prava na privatnost. Generisanje ovih drugih se vrši usled mogućnosti: gubitka poverenja javnosti, gubitka poverenja korisnika proizvoda ili usluga, naknadnog usaglašavanja sa zakonom, pokretanja pravnih postupaka protiv organizacije i naknade šteta nanetih pojedincima usled povrede njihovog prava na privatnost. Sagledavanje rizika predstavlja veoma složen posao čemu najviše doprinosi svrha njegovog obavljanja čija je suština vrlo jednostavna. Svrha procene rizika je da se razume šta su opasnosti. (Oetzel, 2012)

Zbog njihove prikrivenosti česti su previdi, potcenjivanje ili precenjivanje što ni u jednom slučaju nije poželjno. Prvi korak kod procene rizika je da se identifikuju uslovi koji mogu opteretiti ili kompromitovati zaštitu privatnosti i ličnih podataka. (Davies, 2012)

Drugi korak je da se odredi kontrola, opcije i alternative koje mogu pomoći da se smanje, ublaže ili otklone identifikovani rizici privatnosti i zaštite podataka. (De Hert, 2012)

Iz tih razloga izvodimo zaključak da je prilikom sagledavanja rizika neophodna saradnja pravnika, inženjera, dizajnera i menadžera s obzirom na različita razmišljanja i poglede na problematiku u vezi sa njima. To je sasvim prirodno jer je opštepoznato da su pravno, inženjersko i organizacijsko veoma različita gledišta utemeljena na potpuno drugačijim osnovama. Nesebična saradnja i prožimanje svih navedenih aspekata može pravilno usmeriti definisanje zaštite i zaštitnih mera i stvoriti povoljnu osnovu za njenu buduću primenu ali i unapređivanje i razvoj. Međutim, pre nego što se stvore uslovi za

bavljenje zaštitom takva saradnja može dovesti do kompetentnog sagledavanja svih vrsta rizika koji prate određenu delatnost. Uopšteno gledano njihov broj je veliki ali se racionalizacijom koja je u biti sučeljavanja različitih gledišta, na bazi pune kooperativnosti, mogu iskristalisati oni od značaja čiji je broj znatno manji. U tom kontekstu se može analizirati i poslovanje, u Republici Srbiji (nadalje RS) prisutnih telekomunikacionih operatora, zasnovano na pružanju telekomunikacionih usluga, kao delatnosti u okviru koje je obrada ličnih podataka nužnost i izuzetno frekventna pojava. Između ostalih jedan od rezultata opisane saradnje u konkretnom slučaju, u najopštijem obliku, bez bilo kakvog detaljisanja bio bi identifikacija i realna procena svih rizika od značaja za ovu oblast poslovanja, koji će upravo zbog toga biti ukratko prezentovani.

2.1 Rizik krađe identiteta

Jedan od uvek prisutnih rizika kada je u pitanju zaštita podataka o ličnosti jeste krađa identiteta. Prikupljanje podataka o ličnosti usko je povezano sa upotrebom odnosno obradom identifikacionih dokumenata pojedinca. Postupanje sa ovim dokumentima se uvek svodi na prepisivanje podataka iz njih, njihovo očitavanje, fotokopiranje ili skeniranje što najčešće isključuje selektivnost i doslovce znači da se u celosti preuzimaju lični podaci fizičkih lica sadržani u njima. Kako ti podaci potpuno određuju njihov identitet, navedene radnje u vezi sa postupanjem sa istima vrlo često mogu biti uzrok ozbiljnih problema. Tome naročito doprinosi razvitak tehnologija u svim oblastima savremenog delovanja čoveka. Iako je taj razvitak neporecivo nosilac napretka sa jedne strane, sa druge strane može delovati kontraproduktivno i direktno uticati na smanjenje efikasnosti i mogućnosti preventivnog suzbijanja ili eliminacije pomenutih problema.

2.2 Rizik prikupljanja nesrazmernog svrsi

Činjenica izneta u opisu prethodne vrste rizika, da se vrši potpuno preuzimanje ličnih podataka iz identifikacionih dokumenata, nam govori da se takvim postupkom direktno generiše potencijalno nova vrsta rizika, koji se upravo iz tog razloga naziva prikupljanje nesrazmerno svrsi obrade. Uzimanjem svih u tretiranom dokumentu sadržanih podataka, što direktno nameće priroda samih radnji kakve su fotokopiranje ili skeniranje, uzimaju se i podaci koji nisu potrebni za deklarisanu svrhu obrade. Ovu vrstu rizika ne treba poistovećivati sa mnogo zastupljenijim vrstama, kada je obrada podataka u pitanju, kao što su: rizik neodređene svrhe obrade i rizik obrade koji prevazilazi deklarisanu svrhu. Njena tipična karakteristika ili najbitnija razlika u odnosu na ove vrste rizika jeste u tome što namera nije izražena ali je potencijalno prisutna i može se ispoljavati u najraznovrsnijim oblicima i varijantama.

2.3 Rizik neadekvatnog pristupa podacima

Ovu vrstu rizika sam naziv najbolje odražava, međutim vrlo često se poistovećuje i sa neovlašćenim pristupom jer u krajnjoj liniji to bude njegov ishod. Nije posledica, kako to obično biva, nepostojanja organizacionih procedura za pristup ličnim podacima. Svi rukovaoci koji vrše pristup su ovlašćeni ali je njihov pristup izvesnom broju ličnih podataka nepotreban i nije neophodan za radne aktivnosti za koje su zaduženi. Jednostavno, to navodi na činjenicu da procedure koje omogućavaju pristup imaju svoje nedostatke. Oni se ispoljavaju usled neizgrađenog sistema selekcije, čiji bi osnovni zadatak bio definisanje odgovarajućih grupa rukovalaca i omogućavanje pristupa istima najminimalnijem broju podataka neophodnih za rad i adekvatnih njihovim poslovima i zaduženjima. Na taj način bi se izbegla situacija da značajan deo osoblja organizacije, vlasnika zbirke ličnih podataka, dolazi u poziciju upoznavanjanja sa osetljivim podacima o pojedincu, bez definisane potrebe, što se može podvesti i pod aspekt neovlašćenog pristupa.

3 PRAKSA OPERATORA U OBLASTI TELEKOMUNIKACIJA

Poznato je da su telekomunikacije u toku zadnje dve decenije u čitavom svetu, pa posledično i u RS, doživele veliku ekspanziju i da predstavljaju jednu od najprofitabilnijih delatnosti. Nekada jedinstveni servis fiksne telefonije (po tehnološkom zastarevanju telegrafije) dobija svoje

konkurente u mobilnoj telefoniji, internetu i multimediji. Takođe i „Telekom Srbija" kao jedini operator u oblasti telekomunikacija u RS gubi monopol i dobija konkurente kako strane tako i domaće. Spektar usluga koje se mogu pružati u ovoj delatnosti je zahvaljujući takvom razvoju događaja veoma proširen kao i broj njihovih potencijalnih korisnika. Kao što je opštepoznato svako pravno ili fizičko lice može iskazati potrebu i po sopstvenoj volji se opredeliti za neki od nabrojanih servisa, pa od telekomunikacionog operatora koji poseduje isti zahtevati pružanje usluga. Tom širenju umnogome doprinose i marketinške aktivnosti operatora, koje se sve više intenziviraju, kao presudan faktor uspešnog i održivog poslovanja. U takvom poslovnom ambijentu se svakodnevno dešava ogroman broj kontakata i interakcija između potencijalnih korisnika i pružalaca, koji ima tendenciju stalnog povećanja.

Za inicijaciju ostvarenja iskazanih želja ili potreba do skoro je bilo neophodno posetiti korisnički servis odabranog telekomunikacionog operatora i popuniti odgovarajući zahtev. Tom prilikom se iz identifikacionih dokumenata fizičkih lica, na koja ćemo se ograničiti u ovom radu, prepisivanjem vršio prenos njihovih ličnih podataka u zahtev. Zahtev je potom prosleđivan odgovarajućim službama operatora radi dalje obrade. Trenutno je ovaj uobičajeni postupak nešto izmenjen zahvaljujući tehnološkom napretku, pa se umesto prepisivanja podataka vrši njihovo očitavanje elektronskim čitačima. Međutim tehnološkim unapređenjima je suštinski promenjen samo način prikupljanja podataka i ništa više.

Procedure po kojima se dalje postupa su definisane Opštim uslovima za zasnivanje pretplatničkog odnosa koje sačinjava i poseduje svaki operator iz domena ove delatnosti (u bibliografiji date URL adrese gde se nalaze Opšti uslovi reprezentativnih telekomunikacionih operatora u RS sa obrascima koji se koriste kod zasnivanja pretplatničkog odnosa). (Telekom, 2015), (Telenor, 2015), (Vipmobile, 2015), (SBB, 2015), (Orion, 2015)

Pri sačinjavanju ovih uslova kojima se definišu međusobni odnosi korisnika usluge i njenog pružaoca za vreme trajanja pretplatničkog odnosa operator se pridržava Zakona o telekomunikacijama i Zakona o elektronskim komunikacijama. Zato su sa vrlo malim i beznačajnim razlikama pomenute procedure zastupljene kod svih značajnijih operatora i odvijaju se na način opisan u produžetku teksta. Po očitavanju ličnih podataka fizičkog lica, isti se pridružuju namenski formiranoj zbirci podataka, memorisanoj u informacionom sistemu operatora koja se stalno dopunjuje, uvećava i ažurira. Nakon razmatranja zahteva u smislu iznalaženja mogućnosti za njegovu realizaciju i pozitivnog ishoda odnosno usvajanja od strane operatora, korisnik (fizičko lice) biva pozvan u korisnički servis radi sklapanja ugovora o pružanju usluge i detaljnog definisanja međusobnih ugovornih obaveza. Tom prilikom se od korisnika zahteva identifikacioni dokument (lična karta) koji se fotokopira a potom se napravljena fotokopija pridružuje potpisanom ugovoru. Osim uzimanja podataka iz identifikacionog dokumenta u praksi je telekomunikacionih operatora da dodatno zatraže i neke druge lične podatke kao što su državljanstvo, zaposlenje, funkcija itd., koji se ne mogu nikako dovesti u vezu sa zahtevanim uslugama. Na kraju se po sklapanju ugovora, na osnovu istog, vrši unos ugovornih odnosno svih podataka sadržanih u njemu. Osim ličnih ove podatke čine i tehnički, finansijski i drugi i na taj način se dopunjuje zbirka podataka u koju su već uneti prilikom podnošenja zahteva, određeni lični i eventualno neki drugi podaci.

U telekomunikacionim informacionim sistemima (TIS) operatora figurišu zbirke podataka na kojima se zasniva poslovanje operatora i bez kojih je isto nezamislivo. Ono što je posebno simptomatično jeste što ih čine sveukupni podaci vezani za svakog korisnika usluga kao činioca odnosno sastavnog elementa zbirke. U njima nema posebnog izdvajanja ličnih podataka od ostalih podataka koji se odnose na pružanu uslugu (tehničkih i drugih podataka). Međutim u okviru tih osnovnih, nosećih zbirki, kao celine, postoje manje zbirke zasnovane na određenom skupu srodnih podataka. One su u mnogim slučajevima višestruko povezane, po različitim kriterijumima ili parametrima, kako sa osnovnom zbirkom tako i međusobno pa je svaka izolovanost ličnih podataka prividna. Znači da svako stručno lice koje učestvuje u pružanju usluge, radi potreba koje nameće trajno održavanje sistema

(otklanjanje eventualnih kvarova, podešavanje parametara koji se odnose na kvalitet servisa, ažuriranje podataka vezanih za saobraćaj i naplatu), može pristupiti ne samo neophodnim nego svim u zbirci sadržanim podacima korisnika usluge. Ako uzmemo u obzir da je pružanje usluga veoma kompleksan posao, broj stručnih lica koja učestvuju u njemu je posledično veliki, tako da su i lični podaci korisnika nepotrebno dostupni velikom broju rukovalaca zbirkama podataka. Bez obzira što su svi podaci o korisnicima usluga podvedeni pod okrilje službene tajne, rizik od krađe identiteta u ovakvim uslovima je ogroman. Takođe i rizici zbog prikupljanja podataka nesrazmernog deklarisanoj svrsi i neadekvatnog pristupa podacima imaju veoma visoke nivoe. Možemo konstatovati da su uzrok tome neadekvatne procedure i njima predviđeni postupci telekomunikacionih operatora koji su nam u ovom slučaju poslužili kao primer. Da mogu biti s pravom reprezent stanja u našoj zemlji, kada je u pitanju pravo na privatnost i zaštita podataka o ličnosti, omogućile su činjenice da su telekomunikacije u neprestanoj ekspanziji i da podrazumevaju permanentno rukovanje ličnim podacima. Sudeći po izloženom načinu prikupljanja i rukovanja ličnim podacima sopstvenih korisnika, kako postojećih tako i potencijalnih, možemo oceniti da je stanje u našoj zemlji zabrinjavajuće i podložno kritici. Takva kvalifikacija se nameće bez obzira što i krađa identiteta, kao jednog od najopasnijih vidova zloupotrebe ličnih podataka, nije u RS česta pojava kao u nekim razvijenim zemljama i što tehničko-tehnološki stepen razvijenosti ne pruža mogućnosti za takve aktivnosti kao u njihovom slučaju. Takva trenutna situacija ne umanjuje obavezu da se zaštiti ličnih podataka i pravu na privatnost treba pridavati veća pažnja. U prilog tome ide činjenica da u konkretnom slučaju, prisustvo identifikovanih rizika znači postojanje potencijalno velikih mogućnosti za otuđenjem i širenjem ogromnih količina ličnih podataka o pojedincima van okvira organizacije i poslovanja operatora koji ih poseduje. Svako zanemarivanje zaštite podataka ili njeno potiskivanje u drugi plan, povećava identifikovane rizike i verovatnoću eventualnog prenošenja ili otuđenja podataka u smeru ka drugim organizacijama ili pojedincima i progresivno komplikuje situaciju. U tom slučaju pojavljuju se i ostale poznate vrste rizika a vrlo često i neke nove koje nastaju njihovim kombinovanjem.

4 MOGUĆNOSTI ELIMINACIJE

Konkretne mere koje bi trebalo preduzeti u cilju smanjenja navedenih rizika i približavanja razvijenom svetu jesu pre svega tehnološke. Neophodno je obezbediti bolja softverska rešenja u primenjivanim aplikacijama, bilo razvojem u sopstvenoj režiji bilo kupovinom od renomiranih kuća, koja bi omogućila potpuno odvajanje ličnih od ostalih podataka. Tako bi se kreirale posebne zbirke podataka i to sa ličnim podacima korisnika i sa podacima koji se odnose na usluge koje se pružaju korisniku. Pri tome se ne može iz okvira ove druge zbirke podataka potpuno isključiti prisustvo najminimalnijeg broja pojedinih ličnih podataka na osnovu kojih se može vršiti isključivo identifikacija korisnika usluge.

Ovakvo postupanje bi omogućilo i unapređenja u organizacijskom smislu. Šifre za pristup tako kreiranim zbirkama podataka bi bile nezavisne čime bi se izbegla dosadašnja situacija da se dodelom šifre za pristup po automatizmu omogućava pristup ličnim podacima. Na ovaj način bi se već u startu znatno ograničio broj lica koja mogu pristupiti ličnim podacima korisnika. Licima kojima bi to bilo omogućeno bi bila nametnuta veća odgovornost u skladu sa aktuelnom pravnom regulativom u RS kao i aktima poslovnog sistema odnosno operatora telekomunikacionih usluga.

Takođe bi bilo neophodno okupiti na jednom mestu stručnjake iz oblasti pravne, inženjerske i organizacijske struke i sučeljavanjem mišljenja doći do zaključaka koji su to minimalno potrebni podaci koje treba prikupljati od korisnika. Time bi se izbegla obrada suvišnih podataka, štedeli resursi sistema i izbeglo nepotrebno gubljenje vremena.

Jedna od mera koja bi stvorila preduslove za značajne pomake u ovoj oblasti je donošenje novog Zakona o zaštiti podataka o ličnosti usaglašenog sa konvencijama i direktivama EU. Takav novi Zakon o zaštiti podataka o ličnosti bi bio osnova za donošenje sektorskih zakona, koji bi se detaljnije pozabavili ovom problematikom.

Takođe bi omogućio i usklađivanje ostalog zakonodavstva koje se odnosi na određene oblasti delovanja a koje iziskuju rad sa podacima o ličnosti.

Naravno, rizici koji su bili predmet ovoga rada sveli bi se na prihvatljiviju meru ili bi pojedini čak mogli potpuno izgubiti na značaju što je sasvim razumljivo s obzirom na posledično eliminisanje uzroka njihovog egzistiranja.

5 ZAKLJUČAK

Trenutno u Republici Srbiji postoji politička opredeljenost za pridruživanje Evropskoj uniji i rad vlasti je usmeren na ispunjavanje za to potrebnih uslova. Sigurno je da se među potrebnim uslovima nalazi i onaj koji se odnosi na pravnu regulativu u zemlji. Njen sastavni deo svakako je, između ostalog i Zakon o zaštiti ličnih podataka utemeljen na pravu na privatnost svakog pojedinca. Iako u EU ne postoji potpuna ujednačenost kada je u pitanju pravna regulativa, pred našom zemljom je ozbiljan posao kako bi se u tom pogledu smanjio raskorak u odnosu na nju. Preuzimanje pozitivnih iskustava i odgovarajućih akata iz EU može biti samo prvi korak na tom putu. Inače okvir za donošenje smernica u EU je takođe pripreman sistematizovanjem i sumiranjem pozitivnih iskustava razvijenih zemalja širom sveta čiji je ishod izdvajanje najboljih elemenata. (Wright, 2011)

Međutim neophodno je mnogo više učiniti, kako kroz tehničko-tehnološki razvoj zemlje tako i podizanjem opšte kulture kada je zaštita podataka o ličnosti u pitanju. Da bi efekat bio potpun takve aktivnosti se trebaju spustiti na nivo najmanjih poslovnih sistema ili organizacija. Ovakve težnje treba da nastaju sa nastankom organizacija i moraju se implementirati u njihove organizacione kulture. U tom smislu veliki doprinos mogu dati pojedini koncepti nastali u razvijenom svetu u kome su zahvaljujući njima postignuti značajni pozitivni rezultati. Mnogi od njih su zasnovani na ideji da se korisnik mora postaviti u centar.

To može biti preporuka svakom od operatora, kako u telekomunikacijama tako i u drugim oblastima, pa i uopšte svim poslovnim sistemima koji poseduju zbirke podataka i rukuju istima, koji delatnost obavljaju u Republici Srbiji, da korisnik i kod njih mora biti u centru i da on predstavlja osnovni elemenat svrhe njihovog postojanja. U tom kontekstu se posmatra sve što je vezano za korisnika proizvoda ili usluga uključujući i njegovo pravo na privatnost i svaki podatak koji se odnosi na njegovu ličnost. U tu svrhu treba razvijati sofisticiranije sagledavanje praktične i političke realnosti i uzimati ih u obzir kada se procenjuju, čitaju i koriste izveštaji studija uticaja na privatnost. (Waters, 2012)

U svakom slučaju, bez obzira na to da li će se pridruživanje dogoditi ili ne, opšti je interes da se problematika ove vrste dobro unapredi, uredi i stavi pod kontrolu. U tu svrhu je preporučljivo angažovati značajne resurse i finansijska sredstva jer je nesumnjivo takva praksa donela dobrobit mnogo većim i razvijenijim zemljama što može biti smernica za našu zemlju na putu da postane razvijena i moderna država.

CITIRANI RADOVI

Cavoukian, A. (2011). *Privacy by Design in Law, Policy and Practise.* Ontario: Information and Privacy Commissioner.

Davies, S. H. (2012). *Empirical research of contextual factors affecting the introduction of PIA frameworks in the Member States of the Eupopean Union.* Brussels: PIAF.

De Hert, P. K. (2012). Recommendations for a privacy impact assessment framework for European Union. Brussels-London: PIAF.

Oetzel, M. C. (2012). Privacy-by-Design through systematic privacy impact assessment-presentation of a methodology. *PRIVACY-BY-DESIGN THROUGH SYSTEMATIC PRIVACY IMPACT ASSESSMENT - A DESIGN SCIENCE APPROACH* (str. 6). Barzelona: 20th European Conference on Information Systems (ECIS 2012).

Orion. (2015). Preuzeto sa http://oriontelekom.rs/orion telekom/o nama/opsti uslovikoriscenja.299.html

SBB. (2015). Preuzeto sa http://www.sbb.rs/upload/document/d3i opsti uslovi 20140725.pdf

Telekom, S. (2015). Preuzeto sa http://open.telekom.rs/home/General.aspx?temp=20

Telenor, S. (2015). Preuzeto sa https://www.telenor.rs/media/TelenorSrbija/Opšti-uslovi-univerzalniservis.pdf

Vipmobile, S. (2015). Preuzeto sa http://www.vipmobile.rs/upload/documents/Opšti-uslovi-jun-2015.pdf

Waters, N. (2012). Privacy Impact Assessment - Great potential not often realised. U D. D. Wright, *Privacy Impact Assessment* (str. 11). Dordrecht: Springer.

Wright, D. W. (2011). *A Privacy Impact Assessment Framework for Data Protection and Privacy Rights.* Dordrecht: PIAF.

Zajić, A. (2015). Gde su granice lične (ne)privatnosti. *Biznis i finansije*, 74.

Zakon. (2008). Zakon o zaštiti podataka o ličnosti. *Službeni glasnik RS*(97). Preuzeto sa http://www.minrzs.gov.rs/files/doc/porodica/ostali/Zakon%20o%20zastiti%20podataka%20o%20licnosti.pdf

Datum prve prijave: 17.12.2015.
Datum prijema korigovanog članka: 06.03.2016.
Datum prihvatanja članka: 14.03.2016.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*
Šćekić, D. (2016, July 15). Neki rizici kod zaštite podataka o ličnosti i mogućnosti njihove eliminacije. (Z. Čekerevac, Ed.) *FBIM Transactions, 4*(2), 157-164. doi:10.12709/fbim.04.04.02.16

*Style – **Chicago** Sixteenth Edition:*
Šćekić, Draško. 2016. "Neki rizici kod zaštite podataka o ličnosti i mogućnosti njihove eliminacije." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 4 (2): 157-164. doi:10.12709/fbim.04.04.02.16.

*Style – **GOST** Name Sort:*
Šćekić Draško Neki rizici kod zaštite podataka o ličnosti i mogućnosti njihove eliminacije [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Belgrade : MESTE, July 15, 2016. - 2 : Vol. 4. - pp. 157-164.

*Style – **Harvard** Anglia:*
Šćekić, D., 2016. Neki rizici kod zaštite podataka o ličnosti i mogućnosti njihove eliminacije. *FBIM Transactions,* 15 July, 4(2), pp. 157-164.

Style – **ISO 690** Numerical Reference:
Neki rizici kod zaštite podataka o ličnosti i mogućnosti njihove eliminacije. **Šćekić, Draško.** [ed.] Zoran Čekerevac. 2, Belgrade : MESTE, July 15, 2016, FBIM Transactions, Vol. 4, pp. 157-164.